CLAIMS

1. A data archiving system for a storage device (10) arranged to communicate with an archival device (40) and to upload a file (30) thereto, wherein the storage device (10) is arranged to generate a file encryption key (100) and encrypt the file (30) with the file encryption key upon upload to the archival device (40), the file encryption key (100) being regeneratable by the storage device (10) upon presentation of the encrypted file (30').

2. A data archiving system according to claim 1, wherein the storage device includes a private encryption key, the file encryption key (100) being generated in dependence on a randomly generated number (120) and the private encryption key, wherein the randomly generated number (120) is stored in a header (410) to the file (30) upon uploading.

3. A data archiving system according to claim 1, wherein the storage device (10) includes a private encryption key and a file encryption key database, the file encryption key (100) being generated in dependence on the private encryption key, wherein data necessary to generate a decryption key to decrypt the encrypted file (30') is written to the file encryption key database upon uploading.

4. A data archiving system according to claim 3, wherein data to match the encrypted file (30') to the data necessary to generate a decryption key is written to the encryption key database upon uploading.

5. A data archiving system according to claim 1, wherein the storage device (10) includes a file encryption key database, wherein the file encryption key is written to the file encryption key database upon uploading.

6. A data archiving system according to claim 5, wherein an identifier (413) is written to a header (410) of the file and to the file encryption

key database upon uploading to associate the file encryption key with the encrypted file.

7. A data archiving method comprising:

generating a file encryption key;

encrypting a file with the file encryption key; and,

uploading the encrypted file to an archival device;

regenerating the file encryption key upon download of the encrypted file; and,

decrypting the file with the regenerated file encryption key.

8. A method according to claim 7, wherein the step of generating the file encryption key comprises generating the file encryption key in dependence on a randomly generated number and a private encryption key and storing the randomly generated number in a header to the file, wherein the step of regenerating the file encryption key comprises the step of obtaining the randomly generated number from the header to the file and regenerating the file encryption key in dependence on a randomly generated number and the private encryption key.

9. A method according to claim 7, further comprising the step of storing data necessary to regenerate the file encryption key in a file encryption key database.

10. A method according to claim 9, further comprising the step of writing data to the file encryption key database for matching the encrypted file to the stored data necessary to regenerate the file encryption key.

11. A method according to claim 10, further comprising the steps of writing an identifier to a header of the file, the identifier comprising the data for matching the encrypted file to the stored data.

12. A computer program comprising computer program code means for performing all of the steps of any of claims 7 to 11 when said program is run on a computer.

13. A computer program as claimed in claim 12 embodied on a computer readable medium.